FortiAuthenticator

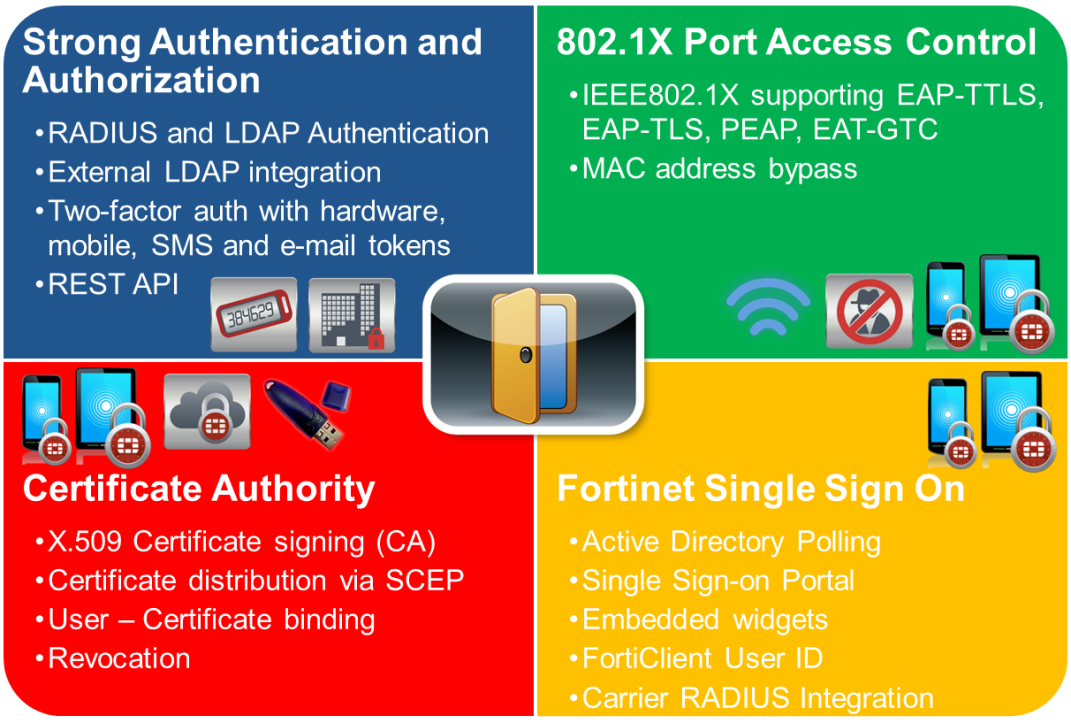
Frequently Asked Questions for Fortinet's FortiAuthenticator Platform

****Document based on features available as of FortiAuthenticator 3.1 GA ****

General FAQs

What is FortiAuthenticator?

FortiAuthenticator is a User Identity Management solution providing a variety of authentication related functions for the Fortinet network infrastructure.



There are four main functions supported by the FortiAuthenticator:

Strong Authentication and Authorization:- FortiAuthenticator supports local and remote authentication via RADIUS and LDAP, incremented with two factor authentication.

802.1X Port Access Control:- IEEE802.1X authentication for Wireless or Port Access control can be incremented with the use of token or certificate base two-factor authentication

Certificate Management: FortiAuthenticator can act as a self-signed root or intermediary certificate authority, generating client certificates for use in EAP (wireless), VPN and other client authentication methods.

Fortinet Single Sign On:- FortiAuthenticator can detect user identity using a wide range of transparent identification and manual authentication methods

These features are closely coupled and complement each other for example:

- Certificate management can be used to generate client certificates for EAP 802.1X wireless authentication.
- Explicit authentication is used by both 802.1X and FSSO features for authenticating users.

Strong Authentication and Authorization FAQs

What Authentication methods are supported?

FortiAuthenticator supports RADIUS and LDAP authentication with both local and remote user databases supported for each.

I already have an LDAP directory containing my user details, can I reuse this?

FortiAuthenticator can provide two-factor authentication whilst proxying the authentication request to a back end LDAP directory (e.g. AD, OpenLDAP and e-Directory). Users can be automatically provisioned on the FortiAuthenticator by querying the LDAP directory.

Do you support other authentication protocols such as Diameter/TACACS+?

No. Diameter and TACACS+ are not currently roadmapped. Should you have a requirement for these features, please feedback through your Fortinet Account Manager.

How does FortiAuthenticator deliver authorization?

FortiAuthenticator supports the use of groups which can be granularly controlled to control authentication to devices. Additionally the addition of RADIUS Vendor Specific Attributes (VSA) based on group membership or directly assigned to the user can be assigned. It is then up to the authentication Auth Client / NAS to utilize this information to authorize the user onto the system. This is documented in the FortiAuthenticator Interoperability Guide for Fortinet and Cisco devices.

See http://docs.fortinet.com/fortiauthenticator/ for more detail.

I use a password so why do I need Two-Factor Authentication?

Passwords need to be memorable to the user and because of this fact, they are often insecure. It is human nature to base passwords on easily guessable words (password, username, username123), keyboard patterns (123456, 1qaz2wsx) or something personal to a user (favorite team, child's name). There is also the risk of disclosure of the password, often through bad practice such as sharing login or the reminder post-it note under the keyboard. Another large, sometimes overlooked risk is the reuse of the same credentials on other sites. Most users have a small number of passwords that they share across multiple sites. Should one become compromised, this puts all other sites at risk.

See http://blog.fortinet.com/rethinking-password-security/ for more detail

Two-factor authentication mitigates this risk by requiring something you know (password) and a one-time password based on something you have (token). When the user logs in, unless they have both the password and the 6 digit PIN from the token, access is denied. Additionally, even if someone was to steal both the password and the PIN, the PIN is only valid for 60 seconds and cannot be reused as it is valid only once. For these reasons, two-fact authentication is essential for log-in to any system containing critical information.

Doesn't FortiGate/FortiToken already do two-factor authentication?

Yes. FortiToken can be used to deliver cost effective two factor authentication to the FortiGate platform at an unprecedented price point. This method allows two-factor authentication to a single FortiGate cluster running FortiOS 4.3, 5.0 and above with only the need for a low cost token (unlike vendor solutions like RSA etc which requires a dedicated Authentication Server).

FortiAuthenticator uses the same FortiTokens to deliver two-factor authentication to any version of FortiOS (including version 4.2 and lower), other Fortinet products and third party devices capable of authenticating via LDAP or RADIUS. This allows for an initial two-factor authentication deployment with FortiGate and FortiToken to be extended to support third party devices at a later date if necessary.

What kinds of tokens are available?

FortiAuthenticator supports one of the widest ranges of token formats in the market with:

- Physical FortiToken 200 OATH compliant TOTP (RFC6238) token using a 60 second time step and 6 digits.
- Software FortiTokenMobile OATH compliant TOTP (RFC6238) token using a 30 or 60 second time step and 6 or 8 digits supporting iOS and Android devices.
- Tokenless e-mail and SMS event tokens
- FortiToken 300 is a PIN protected USB based secure x.509 certificate storage device supporting the PKCS#11 protocol. It can be used to securely request and store certificates for use in, for example, FortiGate IPSEC and SSL VPN environments.

RSA's SecurID seed database was compromised. How do Fortinet protect their token seeds?

Fortinet have taken several steps to remove the risk of token seed compromise. For FortiToken200, the seeds are initially stored in the FortiCare database. When registered via the FortiAuthenticator (or FortiGate), the seeds are removed from the database removing the risk of future compromise. Should the customer require to re-provision the token on another system, this will require a support request so that the seed can be re-provisioned on in the FortiCare database from a secure offline copy of the seed.

With FortiToken Mobile, the seed is only stored transiently in the FortiCare provisioning system between the time that the token has been initially assigned and the seed downloaded. It is possible to configure the maximum tiem that the token can be stored in FortiCare before the token is deleted and re-provisioning is required.

How are the seeds protected once on the FortiAuthenticator?

When stored on the FortiAuthenticator the seeds are stored encrypted using AES256.

What if I do not want Fortinet to manage the token seeds?

Fortinet are aware that some customers do not wish Fortinet to manage the token seeds on their behalf. In this situation there are two options:

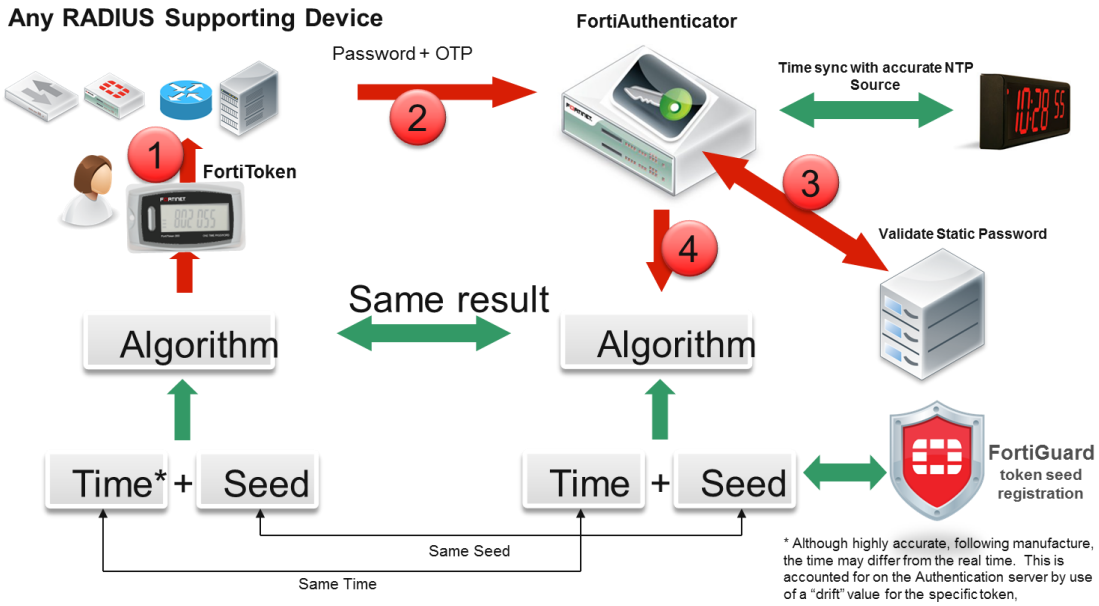
- The seeds can be delivered encrypted on CD and not stored within the FortiCare database. For this, order the FTK200CD-X SKU which comes in 10,20,50 and 100 token versions. For larger options, please contact your Fortinet Account Manager.
- For large deployments, there is also the possibility of self-provisioning the tokens on site. In this case, provisioning tool can be purchased to generate a random seeds and burn them into the memory on the token. For pricing and minimum token volumes, please contact your Fortinet Account Manager.

I have an existing two-factor authentication solution, how can I migrate users to FortiAuthenticator?

FortiAuthenticator supports proxy authentication to existing RADIUS systems including the proxying of challenge-response and any attributes in the responses. This allows FortiAuthenticator to be the primary authentication source with the third party solution and tokens being used. When PAP is used as the authentication protocol, FOrtiAuthenticator can learn the users credentials and automatically provision the users into the local database. Over time,.as the third party tokens expire, users can be migrated to the FortiAuthenticator with minimal effort.

How do TOTP based Two Factor Authenticator Time Functions Work?

FortiToken200 utilizes the open TOTP standard defined in RFC6238 which works as follows:



Step 1 User logs into the FortiGate or third part device (commonly referred to a NAS or in FAC as an Auth Client) using their username and password becomes <password>. They are then challenged for their token passcode.

Pushing the button on the FTK200 will then use the accurate onboard clock, powered by a lithium battery, together with the hardcoded seed to generate a unique passcode.

Step 2 The user enters the token passcode as the challenge field on the NAS/Auth Client which is passed to the FortiAuthenticator.

Step 3 If remote LDAP is configured as the authentication source it is validated, if not, the local password database is checked

Step 4 FortiAuthenticator holds the seed for the token (which has been downloaded from the FortiCare network on initialization) and the time (synchronized via NTP) plus a drift (a measure of the drift of the token time). These values are used to calculate the token passcode.

Step 5 The values are compared and if they match, access is granted, if not, access is denied.

What token drift is allowed?

With the FortiToken 200 and FortiToken Mobile, drifts of ±1 passcode cycle (± 60 seconds) are allowed and automatically adjusted for. Drifts outside of this window will require that the token is manually re-synchronized.

Should there be a major shift in time which makes all tokens become out of sync (most usually caused by enabling NTP after a previously inaccurate time) token sync can be manually shifted en masse.

What devices types can the FortiAuthenticator provide Authentication for?

Any NAS/Auth Client capable of using the RADIUS or LDAP protocols can be integrated with the solution. This includes Fortinet products including administration of all devices, wireless authentication, captive portal authentication and VPN access, most routers, switches, IPSec and SSL VPNs.

Whilst any RADIUS capable device should be able to authenticate, there are 2 ways in which devices can authenticate which have different levels of functionality:

Authentication Method	Description	Support

Password Appended:	User appends to the token passcode to the end of the password e.g.
	
	`Username: <username>`
	`Password: <password><passcode>`
		Supports all RADIUS capable auth clients/NAS devices
		Does not support event tokens such as SMS or Email.

Challenge:	User enters the username and password and the device challenges the user for the token passcode e.g.
	
	`Username: <username>`
	`Password: <password>`
	`Passcode: <passcode>`
		Requires an auth client/NAS device which supports RADIUS Challenge-Response.

Does FortiAuthenticator have an API?

FortiAuthenticator supports a REST API which can be used for multi-factor authentication and passcode only authentication for direct integration with third-party applications. The API is limited to:

- Two factor authentication for the FTK200 and FTM tokens
- One factor authentication of the password or token passcode
- Creation of RADIUS accounting groups
- Creation of users
- Resgistration and provisioning of tokens to users
- Assignment of users to user groups
- Login/out of users in FSSO Database

See the REST API Guide here http://docs.fortinet.com/fauth.html for more details.

Can Windows domain login be two-factor authentication protected?

Yes. A plugin to the Windows credential provider login process is provided, known as FortiAuthenticator Agent for Microsoft Windows. This modifies the authentication process and intercepting the login and requiring entry of the token passcode before the password can be validated. This method also prevents brute forcing of the password since the passcode is required prior to validation of the password. The passcode is validated via the REST API and not RADIUS.

Is password complexity enforcement supported?

User created password complexity can be enforced by:

- Password length
- Number of digits
- Number of characters
- Number of uppercase characters
- Number of symbols

Is user lockout supported?

Yes. A user can be locked out permanently or for a time period based on a configurable number of incorrect logins. Users can also be locked out based on account inactivity, useful for identifying unused accounts.

Is self-service password reset supported?

Yes. Local passwords can be reset via 2 methods depending on the administrative configuration:

- Password reset email
- Answering pre-defined security questions

Is user self-service supported?

Yes. The administrator can create a configurable web page for the user to enter their details before being provided with a username and password. This can be administrator approved or open access.

802.1X Port Access Control FAQs

Is the FortiAuthenticator a NAC solution?

FortiAuthenticator provides some basic elements of a NAC solution, namely port access control.

Does the FortiAuthenticator 802.1X solution support pre / post admission access control.

No. Pre/post admission access control can be performed in conjunction the FortiClient and FortiGate respectively.

Which EAP methods are supported?

FortiAuthenticator supports PEAP, EAP-TTLS, EAP-TLS and EAP-GTC

How are non-interactive devices such as printers supported?

FortiAuthenticator supports MAC Authentication Bypass (MAB) allowing selected devices to automatically authenticate following a failure to interactively provide a username and password.

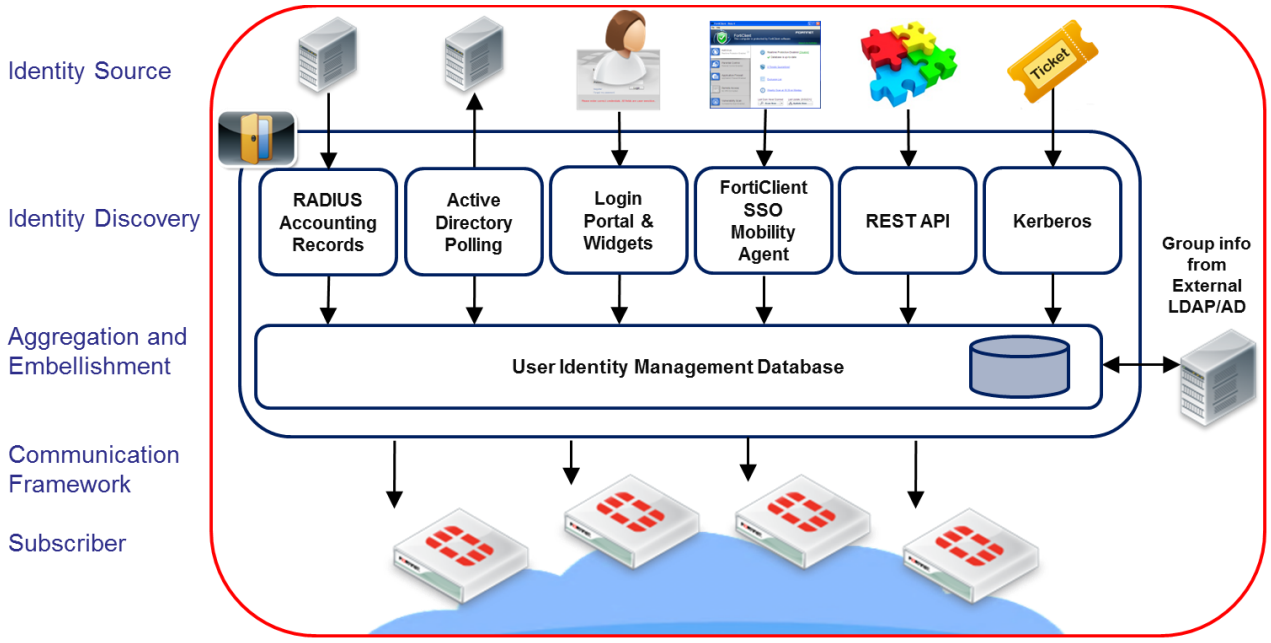
Is Machine Authentication supported?

FortiAtuhenticator integrates with Windows AD so that any Windows machine which has been registered with the Domain and contains machine credentials can perform machine based authentication prior to user based authentication allowing for different networks to be provisioned based on identity and whether the device is approved.

Fortinet Single Sign-On (FSSO) FAQs

How does the FortiAuthenticator FSSO implementation differ from the standard software solution?

Whilst FortiAuthenticator FSSO shares a common origin to the software solution, it has been significantly reworked to deliver a much more rich set of authentication methods.



FSSO is the communication protocol used to deliver user identity information to the FortiGate and FortiCache devices, and is identical to that used but the software solution. Major changes have been made to the collection of user identity information and its embellishment with additionally information such as group membership.

What user identification methods are supported?

FortiAuthenticator supports multiple sources for gathering user identity information including:

Method	Auth Type	Client / Agent Required	Description
Active Directory Polling	Transparent	None	FortiAuthenticator polls Windows Domain Controllers every 5 seconds using Security Event Log Monitoring protocol (over WMI) to detect user login events
Kerberos	Transparent	None	FortiGate redirects the user to the FortiAuthenticator Kerberos portal which authenticates the user with the AD server (KDC) using the Kerberos protocol.
Single Sign-on Mobility Agent	Transparent	Agent	Part of the FortiClient solution. Agent detects login status and user details and communicates information to FortiAuthenticator.
RADIUS Accounting to FSSO	Transparent	None	RADIUS Accounting packets (start, interim and stop) are sent to FortiAuthenticator to identify users
REST API	Transparent/Manual	None	Designed to enable integration with external systems. Allows customer created portals or integration with external authentication systems.
Login Portal	Manual	None	Manual authentication portal. User enters username and password and access is granted until the users selects logout (or until user timeout).
Login Portal with Widgets	Partial Transparent	None	Login portal enhanced with a widget which can be embedded in a users intranet home page. Widget places a cookie in the browser store which is used to transparently authenticate the user on subsequent access.
DCAgent	Transparent	Agent	Agent installs on Domain Controller to detect user login events
TSAgent	Transparent	Agent	Agent installs on Terminal Services or Citrix Server to detect user login events

Is user logout detection supported?

When a user logs out of Active Directory, there is no way to accurately detect this from the Security Event Log. To detect user logout, an additional optional method has been added to poll WMI to detect the logout event and revoke the users access permissions.

Other methods such as Single Sign-On Mobility Agent include logout detection natively as part of the solution.

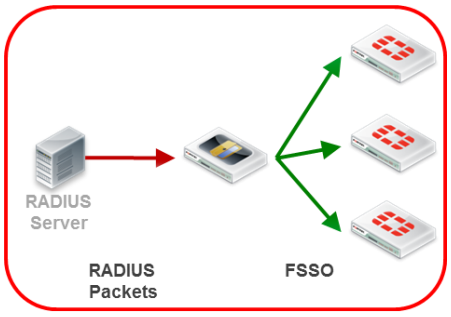
What is the Accounting Proxy and how does it differ from the RADIUS Accounting (FSSO) method?

Both methods are related to single sign on using RADIUS accounting packets but in subtly different ways:

RADIUS Accounting (to FSSO):

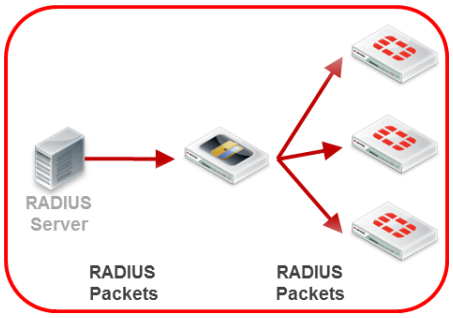
This feature is found under Fortinet SSO Methods > RADIUS Accounting and takes RADIUS Accounting packets from an external RADIUS Server and pushes them into FSSO for use by (multiple) FortiGate and FortiCache devices in Identity Based Policy.

This feature is commonly used to collect identity information from third party wireless controllers.



Accounting Proxy

This feature is found under Fortinet SSO Methods > Accounting Proxy and takes RADIUS Accounting packets from an external RADIUS Server and replays them to multiple FortiGate and FortiMail endpoints for use in RSSO (RADIUS Single Sign On) based policies.



This feature is commonly used to collect identity information in a carrier environment

Certificate Management FAQs

FortiAuthenticator delivers Certificate Authority functionality for the generation of X.509 certificates for multiple uses including (but not limited to):

- VPN security
- Browser/client authentication
- FortiGate Certificates

How can certificates be provisioned to a client?

FortiAuthenticator supports many methods of provisioning certificates including:

- Manual creation by an administrator
- Automatic provisioning via SCEP
- Self provisioning portal which supports provisioning certificates via different methods depending on the device type:
  - iPhone/iPad — Automated SCEP via Mobile Config
  - Android — Manual PKCS#12
  - Windows — PKCS#10 CSR
  - Other — SCEP, PKCS#10 CSR, Manual PKCS#12

Is certificate revocation supported?

Revocation can be managed manually via a CRL or automated via OCSP

How can large scale certificate VPN deployments be supported?

FortiAuthenticator is designed for a large distributed certificate environments for e.g. FortiGate multi-site VPNs. In this environment, there are several features to simplify deployment including:

- Wildcard enrollment
- Support for SCEP
- Integration with FortiManager for distribution of SCEP configuration details to FortiGate devices.

How can I protect my client certificates?

The FortiToken 300 USB Certificate token can be used to securely generate, store and protect your keys and certificates.

- Key is created on, and never leaves the token
- Certificate Signing Request is generated and imported in to the FortiAuthenticator
- FortiAuthenticator signs the CSR and returns the certificate which is imported into the token

Deployment FAQs

What models are available?

The FortiAuthenticator is available in both hardware and VM Formats for the ultimate deployment flexibility.

Hardware

FortiAuthenticator Features/Specs	FortiAuthenticator 200D	FortiAuthenticator 400C	FortiAuthenticator 1000D	FortiAuthenticator 3000D
Maximum users	500	2,000	10,000	40,000
RADIUS Auth auths/sec (Pwd-only)	411	525	628	865
RADIUS Auth auths/sec (FTK 2FA)	339	439	525	643

VM

FortiAuthenticator is supported on VMWare ESXi and operates a stackable license with up to 20 stacked licenses supported. All installations must include the FortiAuthenticator-VM Base license as a starting point.. To increment the user count, any combination of the upgrade licenses can be applied on top of the Base license.

FortiAuthenticator-VM License	Users
FortiAuthenticator-VM Base	100
FortiAuthenticator-VM 100 User Upgrade	+ 100
FortiAuthenticator-VM 1,000 User Upgrade	+1,000
FortiAuthenticator-VM 10,000 User Upgrade	+10,000
FortiAuthenticator-VM 100,000 User Upgrade	+100,000

Greater than 1M+ users are supported, please contact your Fortinet Account Manager for more detail.

Metrics including number of supported Auth Client/NAS devices and number of supported FortiTokens are scaled in proportion to the licensed users. For more details please see the FortiAuthenticator Administration Guide for detail..

How are the FSSO Features Licensed?

The FSSO authentication methods all push their identity information into a shared user database which statefully tracks and updates user identity. The maximum number of users which can be stored in the user database is equal to the max user limit for the device. However, it is possible for a single user to be active on multiple IPs without penalty. This is particularly useful in a BYOD environment where a user may have multiple devices active.

These users are displayed in the FSSO Monitor.

How are users licensed in Accounting Proxy?

The RADIUS Accounting Proxy (which communicates to the FGT/FML via RSSO) does not keep session state or user count. There is no user licensefor this feature, each device is restricted to a RADIUS Packets per second (in plus proxied out) based on the capability of the box e.g.

Note that these users DO NOT show up in the FSSO Monitor.

Will the VM version support other hypervisors?

Other hypervisors are being planned. Should you have such a requirement, please notify the FortiAuthenticator Product Manager.

How can I evaluate FortiAuthenticator?

The most simple method is via the VM platform as this can be facilitated within a matter of days. Hardware is available for evaluation but is limited and may take longer to arrange. Please contact your Fortinet Account Manager to arrange.

Is High Availability supported?

FortiAuthenticator supports Active-Passive high availability:

- Active-Passive: Devices must be installed on the same Layer 2 network. IP address failover occurs so only 1 devices ias active at any time. High Availability for all features is supported in this mode.

Active-Active / Geo HA in final stages of development for version 3.2

- Active – Active Configuration Sync: In version 3.2, FortiAuthenticator will support A-A Ha with geographic separation between the devices, In this mode, a limited subset of data will be synchronized between the devices including:
    - Users
    - Groups
    - Tokens
  - Because of this, this mode is suitable for explicit authentication but other features may be limited e.g.
    - FSSO User Authentication - state not synchronized
    - Failed logins (used for lockout) are not synchronized
    - `Certificates are managed via the Master cluster member only

Are there plans for 8x5 Support?

FortiAuthenticator is deliberately only offered with 24x7 support for good reason. FAC deployment and support is often complicated, requiring support for integration with e.g.

- Multiple flavours of LDAP
- Active Directory
- Windows Desktop (Windows Auth Agent)
- Mobile devices (FTM)
- FortiToken
- IIS (Agent coming soon)
- Multiple flavours of RADIUS (coming soon)

Additionally, most other vendors sell their tokens with per user support however, Fortinet do not. Pricing wise, FAC/FTK is the most cost effective solution available for 2FA and delivers significantly greater features above the competition at the same price point. When you calculate the contribution of FAC to a large token deal, the FAC component is a small amount in comparison. For all of these reasons, 8x5 support will not be offered on FAC.

System FAQs

How do I manage the FortiAuthenticator?

FortiAuthenticator is managed via a HTTPS Management interface. There is an SSH and console based CLI however this is to configure the IP address and default gateway only.

What system monitoring is provided?

FortiAuthenticator supports SNMP v1, v2c and v3 polling and SNMP Traps.

What debugging tools are available?

FortiAuthenticator supports a range of in-built system methods to aid with debugging including:

- Summary and detailed service debug logs
- TAC support debug file download
- Standard debug tools including ping, traceroute nslookup and dig
- TCPDump for packet capture and analysis. This is now available from the GUI.

Competitive FAQs

What is the competition to FortiAuthenticator?

Due to the broad nature of features supported by FortiAuthenticator, it competes with many differing products. In its one role of multi-factor authentication it competes directly with RSA SecureID and ACE, Safenet Account Manager and CryptoCard MAS (Managed Service, now owned by Safenet), Entrust Identity Guard, Vasco.

The FortiAuthenticator key selling points against the competition are:

- **Simplicity: -** RADIUS, LDAP and two-factor authentication supported out of the box with no additional licenses required.
- **Cost: -** Low cost FortiTokens and FortiAuthenticator deliver one of the industry's lowest cost overall solutions whilst maintaining the high quality and functionality associated with Fortinet products
- **Fortinet brand:** - One stop vendor for firewall and two-factor authentication. Fortinet is the security specialist with the highest performance and broadest range of solutions.
- **Upgrade path:** - Customers of FortiGate/FortiToken can extend the solution at any time to authenticate third-party solutions with the FortiAuthenticator using their existing FortiToken investment.
- **Additional features:**- Self-service registration and password reset portals, certificate management and e-mail/SMS token features are included on the system at no additional charge.

The solution also provides RADIUS in a similar fashion to the Juniper Unified Access Control and Cisco Secure Access Control Server, however, FortiAuthenticator provides fully integrated two-factor authentication unlike these providers.

What are the plans for feature development of the FortiAuthenticator product?

The plan for FortiAuthenticator is to become the access control mechanism for the full Fortinet product range. A full roadmap is available on request but please feedback any requirements you may have through your usual channels.